UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,064	01/05/2001	Chiaki Tanimoto	XA-9419	2136

181 7590 10/20/2004

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 10/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/754,064	TANIMOTO ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 January 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/5/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-31 have been examined.

Priority

2. The instant application claims priority to:

Japan Patent Application No. 2000-003295, filed 12 January 2000,

Japan Patent Application No. 2000-003297, filed 12 January 2000,

Japan Patent Application No. 2000-323178, filed 23 October 2000.

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d) for each of the three above named applications, which papers have been placed of record in the file.

Information Disclosure Statement

4. The following Information Disclosure Statement(s) in the instant application has been fully considered:

IDS filed 5 January 2001.

5. A supplemental IDS was filed without a Form PTO-1449 on 7 August 2001, which was solely addressed to clarifying the publication date, in October, 1997, of item

AP disclosed in the IDS filed 5 January 2001. The IDS filed 7 August 2001 has been fully considered.

Drawings

6. The drawings are objected as failing to comply with 37 CFR 1.74 and 37 CFR 1.83 because no reference letters or numerals were used to identify claims elements in figures 4, 7, 8, and 12.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

7. Claims 1 and 10-12 are objected to because of the following informalities: Each claim lacks a transitional phrase. In each claim, it is being presumed that the limitations consist of everything after the word "wherein" and that the limitations are being recited in an open-ended manner. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 9 and 17-31 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for the generation of the computational results, does not reasonably provide enablement for the overflow computation. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make the invention commensurate in scope with these claims. Though microprocessors inherently contain overflow (OV) flags and borrow (BR, the inverse of the carry flag) flags, it is not clear from the specification how the overflow or borrow computation is derived, or under what circumstances the overflow or borrow flag would be set. For purposes of the prior art search, claims 9 and

17 stand or fall with claims 4 and 15, respectively. Claims 18-31 are being evaluated based on their other limitations.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 2-9 and 14-31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 2 and 14, the phrase "or the like" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by "or the like"), thereby rendering the scope of the claim(s) unascertainable. See MPEP § 2173.05(d). For purposes of the prior art search, it is being presumed that the term refers to any cryptographic algorithm.

Claim 3 recites the limitation "the exponential residue multiplying operation" in the first two lines. There is insufficient antecedent basis for this limitation in the claim. For purposes of the prior art search, it is being presumed that claim 3 is dependent on claim 2.

Claim 22 recites the limitation "the ... addresses" on p. 90. There is insufficient antecedent basis for this limitation in the claim.

Claims 4-9, 15-21, and 23-31 depend from rejected claims 2 and 14, and include all the limitations of those claims, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

10. Claims 1-3 and 12-14 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,064,740 to Curiger et al.

As per claims 1, 2, 12, and 13, the integrated circuit disclosed by Curiger incorporates a signal from an oscillator to drive its calculations for RSA on a co-processor (see column 9, lines 33-61).

As per claims 3 and 14, Curiger discloses an exponential residue multiplying operation run on a co-processor, which is inherently invoked using instructions on the CPU (see column 7, line 43 to column 8, line 15).

11. Claims 10 and 11 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 4,179,657 to Hobbs.

Hobbs discloses an anti-jamming communication system wherein the transmitting of a secure message uses a delay in the duty cycles, so as to create transmissions at irregular intervals (see column 6, lines 1-20).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 4-6, 8, 9, 15-18, 20-24, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,064,740 to Curiger et al. as applied to claim 3 above, and further in view of Schneier, "Applied Cryptography," 1996, pp.248-249.

Regarding claims 4, 9, 15, and 17 the system disclosed by Curiger outputs as an example the result of A^2B mod N if the input is 1, and A^2 mod N if the input is 0.

Curigier further discloses that the system is simply designed to perform different calculations depending upon the current exponent bit (see column 10, line 9 to column 11, line 25). Regarding claim 18, Curiger does not disclose the incorporation of an inverse calculation. The mapping of modulo algorithms to the values of the input bits is arbitrary.

Schneier discloses that it is necessary to solve for ax mod n = b and calculate inverses when deriving a reduced set of residues, which appear is some public-key algorithms (see pp.248-249).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Curiger to return $A^{2'}$ mod N for an input of 1 and AX mod N and to incorporate inverses, as disclosed by Schneier, for an input of 0, in order to derive factors for public-key algorithms.

Regarding claim 5, the result is derived in part from the high order bit of Y (e_i) and the result is stored in a register (see column 11, lines 41-44). The write strobe is invoked by the processor when writing to a register in systems not having a read/write buffer between the register and the bus.

Regarding claim 6, Official Notice is given that it is well-known in the art to use a read-write buffer for performing I/O to a register, the writing to which is controlled by the processor, in order to free the processor from having to monitor asynchronous events related to the enabling of the register for writing.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a read/write buffer, the writing to which is controlled by

the processor, in order to free the processor from having to monitor asynchronous events related to the enabling of the register for writing.

Regarding claims 8 and 16, it would follow that a computation selected would correspond to the most recent bit tested.

Regarding claims 18, 20-23, all microprocessors have OV flags. Official notice is given that the subtraction of a value to normalize a result in an overflow condition is well-known in the art.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to normalize a result, in order to remedy an overflow condition.

Additionally, it is common to store both results of a calculation, such as the alternative overflow adjustments, pending resolution of a bit test, in order to save execution time in pipelined microprocessor architectures.

Regarding claims 24 and 31, a borrow flag is used for the same calculations as the overflow flag, so it would be obvious to apply the same logic it the BR flag as to the OV flag.

13. Claims 7, 19, and 25-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,064,740 to Curiger et al. in view of Schneier, "Applied Cryptography," 1996 as applied to claims 4, 14, and 18 above, and further in view of U.S. Patent No. 4,179,657 to Hobbs.

Curiger and Schneier do not disclose the generation of disturbance data being generated with regular data as determined from an input on a bit-by-bit basis.

Hobbs discloses an anti-jamming device wherein regular and dummy data streams are generated using delay circuits according to the bit values of a control signal (see column 5, line 55 to column 6, line 20). Hobbs further suggests that this is done to maintain high reliability during jamming attempts (see column 1, lines 25-33).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Curiger and Schneier by adding the bit-controlled delay circuits, as disclosed by Hobbs, in order to maintain high reliability during jamming attempts.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Japan Patent Publication No. 1-302288 to Kawamura et al. discloses a circuit for performing modulo calculations based upon input bits.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday, Tuesday, Thursday, and Friday from 8:30 AM - 4:30 PM Eastern Time. Beginning 21 October 2004, the telephone number is being changed to (571) 272-3834.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789 (beginning 21 October, (571) 272-3838).

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900 (beginning in October, (571) 272-2100).

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

October 15, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100